

GP 2122

Docket No.: 1086.1138/JDH

#2
OW
5-21-01

UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Giro HIRAI, et al.)
)
Serial No.: 09/785,232) Group Art Unit: 2122
)
) Examiner: Unassigned
Filed: February 20, 2001)

For: **COMPUTER AND COMPUTER READABLE RECORDING MEDIUM ON WHICH PROGRAM IS RECORDED**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

RECEIVED
MAY 16 2001
Group 2100

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-144816
Filed: May 17, 2000.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: May 11, 2001

By:

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
(202) 434-1500



日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年 5月17日

出願番号

Application Number:

特願2000-144816

出願人

Applicant(s):

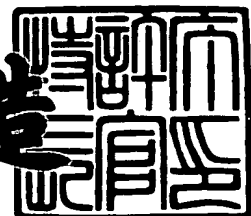
富士通株式会社

RECEIVED
MAY 16 2001
Group 2100

2001年 4月20日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3032326

【書類名】 特許願

【整理番号】 0051098

【提出日】 平成12年 5月17日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/30

【発明の名称】 計算機とコンピュータが読み取り可能な記録媒体

【請求項の数】 9

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 平井 義郎

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 和田 美加代

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 松岡 章一

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 牧山 靖

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 清水 孝紀

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

株式会社内

【氏名】 松下 和弘

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 長瀬 順一

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100095072

【弁理士】

【氏名又は名称】 岡田 光由

【電話番号】 03-3807-1818

【選任した代理人】

【識別番号】 100074848

【弁理士】

【氏名又は名称】 森田 寛

【手数料の表示】

【予納台帳番号】 012944

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707817

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 計算機とコンピュータが読み取り可能な記録媒体

【特許請求の範囲】

【請求項 1】 ネットワークを介して送られてくる、資源とそれを適用させるための適用プログラムとで構成される資源情報を受信し、記憶装置の運用領域に格納する手段と、

上記資源の適用契機に到達したのか否かを判断する手段と、

上記適用契機に到達したことを判断する場合に、上記資源情報を上記記憶装置の保守領域に複写するとともに、次のシステム立ち上げ時に該保守領域が有効化されることになるための処理を行う手段とを備えることを、

特徴とする計算機。

【請求項 2】 請求項 1 記載の計算機において、

上記適用プログラムは、システムの立ち上げにตอบสนองして起動されると、次のシステム立ち上げ時に上記運用領域が有効化されることになるための処理を行うことを、

特徴とする計算機。

【請求項 3】 請求項 2 記載の計算機において、

上記適用プログラムは、上記資源の適用処理後と、その適用処理が失敗する場合に、システム再立ち上げの処理を行うことを、

特徴とする計算機。

【請求項 4】 請求項 1 ないし 3 のいずれか 1 項に記載される計算機において、

上記適用プログラムは、適用の完了した資源情報を、上記運用領域及び上記保守領域から削除する処理を行うことを、

特徴とする計算機。

【請求項 5】 請求項 1 ないし 4 のいずれか 1 項に記載される計算機において、

ハードウェアで構成されるとともに、計算機本体とは別電源で動作して、上記適用プログラムの発行する処理時間情報を受け取り、その処理時間情報を監視す

ることで、上記適用プログラムの動作を監視する管理機構を備えることを、
特徴とする計算機。

【請求項 6】 請求項 5 記載の計算機において、

上記管理機構は、

上記適用プログラムの異常を検出する場合に、次のシステム立ち上げ時に上記運用領域が有効化されることになるための処理を行う手段と、その処理に続けてシステム再立ち上げの処理を行う手段とを備えることを、

特徴とする計算機。

【請求項 7】 請求項 5 又は 6 記載の計算機において、

上記管理機構は、

上記適用プログラムの動作中に発行される計算機本体に対する電源切断要求及びリセット要求を無効化する手段を備えることを、

特徴とする計算機。

【請求項 8】 請求項 5 ないし 7 のいずれか 1 項に記載される計算機において、

上記管理機構は、

上記適用プログラムの異常を検出する場合と、上記適用プログラムから異常通知を受け取る場合と、上記適用プログラムの動作中に計算機本体の電源が切断された場合と、上記適用プログラムの動作中に計算機本体がリセットされた場合に、上記資源の配信元に対して、上記資源の適用失敗を通知する手段を備えることを、

特徴とする計算機。

【請求項 9】 ネットワークを介して送られてくる、資源とそれを適用させるための適用プログラムとで構成される資源情報を受信し、記憶装置の運用領域に格納する処理と、

上記資源の適用契機に到達したのか否かを判断する処理と、

上記適用契機に到達したことを判断する場合に、上記資源情報を上記記憶装置の保守領域に複写するとともに、次のシステム立ち上げ時に該保守領域が有効化されることになるための処理とをコンピュータに実行させるプログラムを記録

したことを、

特徴とするコンピュータが読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを介して配信されてくる資源を所望の適用契機に自動適用させることを可能にする計算機と、それを実現するプログラムを記録したコンピュータが読み取り可能な記録媒体とに関する。

【0002】

計算機では、ファームウェアがバージョンアップする場合、実装されているファームウェアをそのバージョンアップしたファームウェアに更新していく必要がある。このようなファームウェアの更新を自動的に行えるようにする技術の構築が叫ばれている。

【0003】

【従来の技術】

従来では、計算機で使用されるファームウェアがバージョンアップする場合、サービスマンが、そのバージョンアップしたファームウェアと、ファームウェアの交換に用いるプログラムとを記録したCD-ROMなどを持参してユーザの所に出向いて行って、手作業により、そのバージョンアップしたファームウェアと古いファームウェアとを交換することで、ファームウェアをバージョンアップしていくようにしていた。

【0004】

一方、Webサーバの普及に伴って、ユーザは、メーカーにより提供されるソフトウェアの一覧を閲覧して、その中からダウンロードするソフトウェアを選択することで、Webサーバから新たなソフトウェアをダウンロードしてインストールしていくことが行われているが、この場合にも、結局の所、ユーザの手作業によりソフトウェアをダウンロードしてインストールしていくという方法を用いている。

【0005】

【発明が解決しようとする課題】

従来技術のようにサービスマンやユーザの手作業により、ファームウェアなどの資源を計算機に投入するようにしていると、各計算機に対して、投入しなければならない資源を迅速に投入できないという問題点がある。

【0006】

すなわち、サービスマンが出向いたり、ユーザが作業を行わない限り、バージョンアップした資源などを計算機に投入できないことから、各計算機に対して、投入しなければならない資源を迅速に投入できないのである。

【0007】

ある計算機でプログラムなどの資源の異常が検出される場合、メーカは、これに応答してその資源をバージョンアップしていくことになるが、他の計算機でその資源の異常が検出される動作が行われているとは限られないことから、その資源を交換する必要があることに気付かないユーザも多く、これがために、この問題点は更に深刻なものとなる。

【0008】

このようなことを背景にして、本出願人は、特願2000-96557号で、ネットワークに接続される端末から、それらの端末の構成情報を自動収集して、端末への配付対象となる新たな資源が作成されるときに、それらの構成情報から、その新たな資源の配付先となる端末を特定することで、その新たな資源の配付先となる端末に対して、その新たな資源を自動配付していくというリモートメンテナンス技術を開示した。

【0009】

そして、このとき、端末が、自動配付される資源を適用待ちとするのか即実行とするのかを設定して、それに従って、自動配付される資源を適用させていくというリモートメンテナンス技術を開示した。

【0010】

本発明は、この本出願人の開示した技術を一步進めて、ネットワークを介して配信されてくる資源を所望の適用契機に自動適用させることを可能にする新たな計算機の提供と、それを実現するプログラムを記録した新たなコンピュータが読

み取り可能な記録媒体の提供とを目的とする。

【0011】

【課題を解決するための手段】

図1に本発明の概要構成を図示する。

【0012】

図中、1は本発明を具備する計算機、2は計算機1に対して資源とそれを適用させるための適用プログラムとで構成される資源情報を配信する保守管理サーバ、3は計算機1と保守管理サーバ2との間を接続するLANなどのネットワークである。

【0013】

本発明の計算機1は、ブート(Boot)情報などを格納するシステムディスク10と、通常の運用処理を実行する基本OS20と、保守管理サーバ2から配信される資源の適用処理を実行する保守用OS30と、ハードウェアで構成されるとともに、計算機本体とは別電源で動作する管理機構40とを備える。

【0014】

このシステムディスク10は、システム立ち上げ時に、基本OS20を立ち上げるのか保守用OS30を立ち上げるのかについて記述するブート情報を格納するブート領域11と、保守作業処理用に用意される保守用OS領域12と、通常の運用処理用に用意される基本OS領域13とを備える。

【0015】

基本OS20の配下には、保守管理サーバ2から配信される資源情報を受信して基本OS領域13に格納する受信手段21と、保守管理サーバ2から配信される資源の適用契機に到達したのか否かを判断する判断手段22と、判断手段22が適用契機に到達したことを判断する場合に、保守管理サーバ2から配信される資源情報を保守用OS領域12に複写するとともに、次回のシステム立ち上げ時に保守用OS領域12が呼び出されることになるようにとブート情報を書き換える実行手段23とが展開される。

【0016】

この受信手段21／判断手段22／実行手段23は、ブート情報の記述に従っ

て、システムの立ち上げに応答して基本OS領域13から読み出されて展開されることになる。

【0017】

保守用OS30の配下には、保守管理サーバ2から配信される資源31と、その資源31を適用させるための適用プログラム32とが展開される。

【0018】

この資源31及び適用プログラム32は、ブート情報の記述に従って、システムの立ち上げに応答して保守用OS領域12から読み出されて展開されることになる。

【0019】

適用プログラム32は、システムの立ち上げに応答して起動されると、次のシステム立ち上げ時に基本OS領域13が呼び出されることになるとブート情報を書き換える処理を行う。また、適用プログラム32は、資源31の適用処理後と、その適用処理が失敗する場合に、システム再立ち上げの処理を行う。また、適用プログラム32は、適用の完了した資源31の資源情報を、保守用OS領域12及び基本OS領域13から削除する処理を行う。

【0020】

管理機構40は、適用プログラム32の発行する処理時間情報を受け取り、その処理時間情報を監視することで、適用プログラム32の動作を監視する処理を行う監視手段41と、監視手段41が適用プログラム32の異常を検出する場合に、次のシステム立ち上げ時に基本OS領域13が呼び出されることになるとブート情報を書き換える処理を行う書換手段42と、書換手段42の処理に続けてシステム再立ち上げの処理を行う再立ち上げ手段43と、適用プログラム32の動作中に発行される計算機本体に対する電源切断要求及びリセット要求を無効化する処理を行う無効化手段44と、保守管理サーバ2に対して、資源31の適用失敗を通知する処理を行う通知手段45とを備える。

【0021】

このように構成される本発明の計算機1では、受信手段21は、通常の運用処理の実行中に、保守管理サーバ2から配信される資源情報（資源＋適用プログラ

ム)を受信すると、それを基本OS領域13に格納する。そして、判断手段22は、通常の運用処理の実行中に、例えば定期的に、その受信した資源の適用契機に到達したのか否かを判断する。

【0022】

この判断手段22の処理を受けて、実行手段23は、判断手段22が適用契機に到達したことを判断する場合には、受信した資源情報を保守用OS領域12に複写する(書き込む)とともに、次回のシステム立ち上げ時に保守用OS領域12が呼び出されることになるようにとブート情報を書き換える。

【0023】

この後、通常の運用処理が終了し、その後、規定の時刻などによりシステムが立ち上げられる。

【0024】

このとき、ブート情報は保守用OS領域12を指しているので、保守用OS領域12から資源31及び適用プログラム32が読み出されて保守用OS30の配下に展開され、これにより、適用プログラム32が起動されて、資源31を適用するための処理が実行される。

【0025】

適用プログラム32は、起動されると、先ず最初に、次回のシステム立ち上げ時に基本OS領域13が呼び出されることになるようにとブート情報を書き換える処理を行う。

【0026】

続いて、適用プログラム32は、例えば処理フェーズに合わせて、管理機構40に対して処理時間情報を通知しながら、資源31の適用処理を実行して行って、その適用処理を完了すると、システム再立ち上げの処理を行う。

【0027】

このときには、ブート情報は基本OS領域13を指しているので、保守管理サーバ2から配信されてきた新たな資源を使って、通常の運用処理が実行されることになる。

【0028】

そして、適用プログラム 3 2 は、適用の完了した資源 3 1 の資源情報を保守用 OS 領域 1 2 及び基本 OS 領域 1 3 から削除することで、重複する適用処理が実行されないように処理する。

【0029】

この処理構成を採るときに、適用プログラム 3 2 に異常が発生すると、管理機構 4 0 は、次のシステム立ち上げ時に基本 OS 領域 1 3 が呼び出されることになるようにとブート情報を書き換えるとともに、システム再立ち上げの処理を行うことで、適用プログラム 3 2 の処理を代行するとともに、資源 3 1 の適用処理の実行中に電源切断要求やリセット要求が発行される場合にはそれを無効化することで、その適用処理が中断されないように制御する。

【0030】

このようにして本発明の計算機 1 によれば、ネットワークを介して配信されてくる資源を所望の適用契機に自動適用させることが可能になる。

【0031】

更に、この実現にあたって、本発明の計算機 1 では、配信されてきた資源の適用処理に失敗しても、通常の運用処理を継続できるようにする構成を採っていることから、通常の運用処理に影響を与えることがない。

【0032】

【発明の実施の形態】

以下、実施の形態に従って本発明を詳細に説明する。

【0033】

図 2 に、本発明の計算機 1 の一実施形態例を図示する。図中、図 1 で説明したものと同一のものについては同一の記号で示してあり、3 a は保守管理サーバ 2 と計算機 1 との間を接続する LAN である。

【0034】

この図に示すように、保守管理サーバ 2 は、各計算機 1 に対しての保守処理を実行する保守管理アプリ 3 0 0 と、各計算機 1 の最新のハードウェア構成情報を管理するハード構成情報テーブル 3 0 1 と、計算機 1 に配信する更新ファームウェアと、その更新ファームウェアに交換するためのツールとして用意されるファ

ームウェア更新プログラムとからなる保守資源302（どの計算機1に配信するのにかについても管理している）とを備える。

【0035】

保守管理アプリ300は、各計算機1から送られてくる各計算機1の最新のハードウェア構成情報を取得して、ハード構成情報テーブル301に登録する。

【0036】

そして、保守管理アプリ300は、いずれかの計算機1でファームウェアの障害が発生すると、その障害情報を取得して、それを図示しない設計センタに通知することで、その障害の発生したファームウェアの更新を指示し、この指示に回答して作成される更新ファームウェアを取得する。

【0037】

この更新ファームウェアを取得すると、保守管理アプリ300は、ハード構成情報テーブル301を参照することで、その更新ファームウェアの配信先となる計算機1を特定することで保守資源302を作成する。

【0038】

そして、保守管理アプリ300は、例えば定期的に、新しく登録した保守資源302を配信先となる計算機1に配信していくことで、各計算機1に対して、障害の発生したファームウェアをバージョンアップされた更新ファームウェアに更新していくことを指示していくのである。

【0039】

各計算機1は、このようにして保守管理アプリ300から配信されてくる保守資源（更新ファームウェア＋ファームウェア更新プログラム）を受け取ると、配信されてきたファームウェア更新プログラムを使って、自装置で使用している更新前の古いファームウェアを、配信されてきた更新ファームウェアに交換する処理を行う。

【0040】

このファームウェアの交換処理を行うために、本発明の計算機1は、図1で説明したように、通常の運用処理を実行する基本OS20の他に、保守管理サーバ2から配信されてきたファームウェアの適用処理を実行する保守用OS30を備

える構成を採っている。

【0041】

そして、これに合わせて、システムディスク10に、システム立ち上げ時に、基本OS20を立ち上げるのか保守用OS30を立ち上げるのかについて記述するブート情報を格納するブート領域11と、保守作業処理用に用意される保守用OS領域12と、通常の運用処理用に用意される基本OS領域13とを備える構成を採っている。

【0042】

図3に、システムディスク10のデータ構造を図示する。

【0043】

図3(a)はディスク構成を示し、図3(b)はブートセクタ構成を示し、図3(c)はブートセクタの管理するパーティションテーブル構成を示している。このパーティションテーブルで使われている記号の意味を図4に示す。

【0044】

この実施形態例では、保守作業処理用に用意される保守用OS領域12は、システムディスク10の「0x1BE」というアドレスの指すパーティションに展開され、通常の運用処理用に用意される基本OS領域13は、システムディスク10の「0x1CE」というアドレスの指すパーティションに展開されることを想定している。

【0045】

図4に示すように、記号BIで示される部分に「0x80」が登録されているときには、そのパーティションはアクティブとなる。これに対して、「0x00」が登録されているときには、そのパーティションはノンアクティブとなる。

【0046】

これから、図5(a)に示すように、システムディスク10の「0x1BE」というアドレスの指すパーティションのBI部分に「0x00」を書き込み、「0x1CE」というアドレスの指すパーティションのBI部分に「0x80」を書き込めば、基本OS20が立ち上げられることとなる。

【0047】

一方、図5(b)に示すように、システムディスク10の「0x1BE」というアドレスの指すパーティションのBI部分に「0x80」を書き込み、「0x1CE」というアドレスの指すパーティションのBI部分に「0x00」を書き込めば、保守用OS30が立ち上げられることとなる。

【0048】

本発明の計算機1は、図2に示すように、ソフトウェア構成的には、基本OS20の配下で動作する保守アプリ100と、保守用OS30の配下で動作するファームウェア更新プログラム104（保守管理サーバ2から配信されてきたもの）とを備えるという構成を採っている。

【0049】

ここで、基本OS20の配下に展開される保守資源101は、保守管理サーバ2から配信されてきた保守資源302であり、基本OS20の配下に展開されるハード構成情報テーブル102は、保守管理サーバ2に送信するハードウェア構成情報を管理するものである。また、保守用OS30の配下に展開される更新ファームウェア103は、保守管理サーバ2から配信されてきた保守資源302の持つ更新ファームウェアである。

【0050】

保守アプリ100やファームウェア更新プログラム104は、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【0051】

一方、本発明の計算機1は、図2に示すように、ハードウェア構成的には、CPU200と、主記憶201と、システムディスク10と、ACアダプタ203から電源供給（計算機本体とは別ルートの電源供給）を受け取る管理ハード202と、ACアダプタ205から電源供給（計算機本体とは別ルートの電源供給）を受け取るリモート装置制御ハード204と、保守管理サーバ2との通信接続を司るLAN制御ハード206とを備えるという構成を採っている。

【0052】

ここで、ファームウェアを実際に実装するハードディスクやアダプタなどについては図示していない。

【0053】

この管理ハード202は、保守用OS30の配下で動作するファームウェア更新プログラム104の動作を監視して、異常を検出する場合には、必要な対策処理を実行する。また、リモート装置制御ハード204は、図示しないリモート装置からの指示を受け取り、計算機本体の電源制御などの処理を司る装置制御ハード（これから説明する図6の207に示すもの）に対して、電源切断指示やリセット指示を発行する処理を行う。

【0054】

図6に示すように、管理ハード202は、図中の α の信号ラインで、リモート装置制御ハード204により発行される装置制御ハード207に対する装置制御指示を受け取り、図中の β の信号ラインで、その受け取った装置制御指示を装置制御ハード207に中継するという構成を採っている。

【0055】

図7に、管理ハード202の持つハードウェア機構（図6に示すインタフェースコントローラが備える）の一実施形態例を図示する。

【0056】

この図に示すように、管理ハード202は、全体の制御処理を実行する主制御機構400と、ファームウェア更新プログラム104の動作をタイマ監視する時間監視機構401と、手動操作による予期せぬ電源切断やリセット指示が発行されたのか否かを監視する本体監視機構402と、リモート装置制御ハード204及び計算機本体との間のインタフェース処理を司るインタフェース機構403と、保守管理サーバ2との間の通信接続を司るLAN制御機構404と、リモート装置制御ハード204により発行される装置制御ハード207に対する装置制御指示を遮断する装置制御遮断機構405と、ファームウェアの交換処理中であるのか否かを表示するファームウェア更新処理中フラグ406とを備える。

【0057】

図8に、基本OS20の配下で動作する保守アプリ100の実行する処理フローの一実施形態例、図9及び図10に、保守用OS30の配下で動作するファームウェア更新プログラム104の実行する処理フローの一実施形態例、図11及

び図 1 2 に、管理ハード 2 0 2 の主制御機構 4 0 0 の実行する処理の一実施形態例を処理フローの形で示したものを図示する。

【 0 0 5 8 】

次に、これらの処理フローに従って、このように構成される本発明の処理について詳細に説明する。

【 0 0 5 9 】

保守アプリ 1 0 0 は、ブート情報（パーティションテーブル）が基本 OS 領域 1 3 をアクティブにしていることでシステムの立ち上げに応答して起動されると、図 8 の処理フローに示すように、先ず最初に、ステップ 1 で、システムディスク 1 0 の保守用 OS 領域 1 2 に保守資源が格納されている場合には、それを削除する。

【 0 0 6 0 】

後述することから分かるように、システムディスク 1 0 の保守用 OS 領域 1 2 には、更新ファームウェアの適用（古いファームウェアとの交換）に成功した保守資源と、更新ファームウェアの適用に失敗した保守資源とが格納されている可能性があるので、これらの保守資源が格納されている場合には、それを削除するのである。

【 0 0 6 1 】

続いて、ステップ 2 で、自装置のハードウェア構成情報を採取して、それを保守管理サーバ 2 に送信する。上述したように、保守管理サーバ 2 は、このハードウェア構成情報の送信を受けて、新たに作成された更新ファームウェアを取得するときに、それをどの計算機 1 に配信したらよいのかを特定して配信していくように処理することになる。

【 0 0 6 2 】

続いて、ステップ 3 で、システムディスク 1 0 の基本 OS 領域 1 3 に保守資源が格納されているのか否かを判断する。後述することから分かるように、システムディスク 1 0 の基本 OS 領域 1 3 には、更新ファームウェアの適用（交換）に成功した保守資源と、更新ファームウェアの適用に失敗した保守資源と、更新ファームウェアの適用を試みていない保守資源とが格納されている可能性があるの

で、先ず最初に、これらの保守資源が格納されているのか否かを判断するのである。

【0063】

このステップ3の判断処理により、システムディスク10の基本OS領域13に保守資源が格納されていることを判断するときには、ステップ4に進んで、その格納されている保守資源が既に適用の完了したものであるのか否かを判断する。この判断処理は、ステップ2で採取したハードウェア構成情報に従って適用されているファームウェアの版数を取得して、それと基本OS領域13に格納されている更新ファームウェアの版数とを比較することで行う。

【0064】

このステップ4の判断処理で、基本OS領域13に格納されている保守資源が既に適用の完了したものであることを判断するときには、ステップ5に進んで、その適用の完了している保守資源を基本OS領域13から削除する。一方、基本OS領域13に格納されている保守資源が適用の完了していないもの、すなわち、適用に失敗したものや未適用のものであることを判断するときには、このステップ5の処理を省略することで、そのまま適用対象として残すことになる。

【0065】

続いて、ステップ6で、保守管理サーバ2から保守資源が配信されてきたのか否かを判断して、保守資源が配信されてきたことを判断するときには、ステップ7に進んで、その配信されてきた保守資源（図2の101で示すもの）を受け取り、システムディスク10の基本OS領域13に格納する。

【0066】

続いて、ステップ8で、予め設定されるファームウェアの適用契機に到達したのか否かを判断して、到達していないことを判断するときには、ステップ6に戻っていくことで、保守管理サーバ2から配信されてくる保守資源を受け取りつつ、ファームウェアの適用契機に到達するのを待つ。

【0067】

このとき設定されるファームウェアの適用契機には、例えば、次回のシステム立ち上げ時にファームウェアの適用を行うとか、月曜日の9時にファームウェア

の適用を行うとか、月末の17時にファームウェアの適用を行うとか、手動によりファームウェアの適用を行うとかいったものがあり、ユーザが自由に設定することが可能である。

【0068】

このステップ8の判断処理で、ファームウェアの適用契機に到達したことを判断するときには、ステップ9に進んで、適用契機を次のものに更新する。

【0069】

続いて、ステップ10で、システムディスク10の基本OS領域13に保守資源が格納されているのか否かを判断して、保守資源が格納されていないことを判断するときには、そのままステップ6に戻っていくことで、保守管理サーバ2から配信されてくる保守資源を受け取りつつ、ファームウェアの適用契機に到達するのを待つ。

【0070】

一方、ステップ10で、システムディスク10の基本OS領域13に保守資源が格納されていることを判断するときには、ステップ11に進んで、その保守資源をシステムディスク10の保守用OS領域12に複写する。

【0071】

この時点で基本OS領域13に格納されている保守資源には、ステップ5の削除対象から外された適用失敗の保守資源と、新たに配信されてきた保守資源とがあるので、前者については、基本OS領域13から保守用OS領域12へとコピーし、後者については、新たに配信されたきた保守資源が手元（基本OS領域13にも書き込んでいる）にあるので、それを保守用OS領域12にコピーするのである。

【0072】

続いて、ステップ12で、保守用OS領域12がアクティブになるようにとブート情報（パーティションテーブル）が書き換えてから、ステップ6に戻ること、保守管理サーバ2から配信されてくる保守資源を受け取りつつ、ファームウェアの適用契機に到達するのを待つ。

【0073】

このようにして、保守アプリ100は、保守管理サーバ2から配信されてくる保守資源を受け取ってシステムディスク10の基本OS領域13に格納していった、ファームウェアの適用契機に到達すると、前回の適用処理で失敗した保守資源と、前回の適用契機から今回の適用契機の間には配信されてきた保守資源とを保守用OS領域12にコピーするとともに、次のシステムの立ち上げ時には保守用OS領域12がアクティブになるようにとブート情報を書き換えていくように処理するのである。

【0074】

この保守アプリ100によるブート情報の書換処理に従って、次のシステムの立ち上げ時には、システムディスク10の保守用OS領域12に格納される保守資源（更新ファームウェア103＋ファームウェア更新プログラム104）が読み出されることで、図2に示すように、保守用OS30の配下のファームウェア更新プログラム104が起動されることになる。

【0075】

このようにして起動されると、ファームウェア更新プログラム104は、図9及び図10の処理フローに示すように、先ず最初に、ステップ1で、次のステップ2の処理に要する時間から決定する監視時間（例えば2倍の時間）を管理ハード202に通知する。

【0076】

この通知を受け取ると、管理ハード202の時間監視機構401は、タイマ監視処理に入って、その通知された監視時間の間にファームウェア更新プログラム104から次の監視時間が通知されない場合には、ファームウェア更新プログラム104の異常を判断するように処理する。

【0077】

続いて、ステップ2で、基本OS領域13がアクティブになるようにとブート情報（パーティションテーブル）を書き換える。すなわち、次のシステム立ち上げ時には、通常の運用処理となる基本OS領域13がアクティブになるように設定するのである。

【0078】

続いて、ステップ3で、ステップ2の処理を正常終了できたのか否かを判断して、正常終了できなかったことを判断するときには、ステップ13に進んで、管理ハード202に対して異常を通知する。一方、正常終了できたことを判断するときには、ステップ4に進んで、次のステップ5の処理に要する時間から決定する監視時間（例えば2倍の時間）を管理ハード202に通知する。

【0079】

この通知を受け取ると、管理ハード202の時間監視機構401は、タイマ監視処理に入って、その通知された監視時間の間にファームウェア更新プログラム104から次の監視時間が通知されない場合には、ファームウェア更新プログラム104の異常を判断するように処理する。

【0080】

続いて、ステップ5で、チェックサムなどのチェック処理を実行することで、保守用OS領域12から読み出した更新ファームウェア103の妥当性をチェックする。

【0081】

続いて、ステップ6で、ステップ5の処理を正常終了できたのか否かを判断して、正常終了できなかったことを判断するときには、ステップ13に進んで、管理ハード202に対して異常を通知する。一方、正常終了できたことを判断するときには、ステップ7に進んで、次のステップ8の処理に要する時間から決定する監視時間（例えば2倍の時間）を管理ハード202に通知する。

【0082】

この通知を受け取ると、管理ハード202の時間監視機構401は、タイマ監視処理に入って、その通知された監視時間の間にファームウェア更新プログラム104から次の監視時間が通知されない場合には、ファームウェア更新プログラム104の異常を判断するように処理する。

【0083】

続いて、ステップ8で、更新ファームウェア103の更新対象となるハードウェア（アダプタなど）を検索する。

【0084】

続いて、ステップ9で、ステップ8の処理を正常終了できたのか否かを判断して、正常終了できなかったことを判断するときには、ステップ13に進んで、管理ハード202に対して異常を通知する。一方、正常終了できたことを判断するときには、ステップ10に進んで、次のステップ11の処理に要する時間から決定する監視時間（例えば2倍の時間）を管理ハード202に通知する。

【0085】

この通知を受け取ると、管理ハード202の時間監視機構401は、タイマ監視処理に入って、その通知された監視時間の間にファームウェア更新プログラム104から次の監視時間が通知されない場合には、ファームウェア更新プログラム104の異常を判断するように処理する。

【0086】

続いて、ステップ11で、ステップ8で検索したハードウェアの持つ古いファームウェアを更新ファームウェア103に交換することで、更新ファームウェア103を適用する処理を実行する。

【0087】

続いて、ステップ12で、ステップ11の処理を正常終了できたのか否かを判断して、正常終了できなかったことを判断するときには、ステップ13に進んで、管理ハード202に対して異常を通知する。

【0088】

そして、ステップ12で正常終了できたことを判断し、あるいは、ステップ13の処理を終了すると、ステップ14（図10の処理フロー）に進んで、管理ハード202に対して監視停止を通知し、続くステップ15で、システム再立ち上げのリブート処理（リセット処理）を実行して、処理を終了する。

【0089】

このようにして、ファームウェア更新プログラム104は、先ず最初に、基本OS領域13がアクティブになるようにとブート情報を書き換えてから、処理フェーズ毎に、その処理フェーズに入る前に監視時間を決定して管理ハード202に通知してからファームウェア更新の適用処理を実行していった、正常に適用処理を終了できない場合には、その旨を管理ハード202に異常発生を通知しつつ

、最後に、システム再立ち上げのリブート処理を実行していくように処理するのである。

【0090】

ここで、図8の処理フローでは説明しなかったが、保守管理サーバ2から配信されてくる更新ファームウェアの適用が完了していない間に、その更新ファームウェアの改版にあたる次の更新ファームウェアが配信されてくるときには、最新の更新ファームウェアのみが有効なものとなるようにするために、システムディスク10の基本OS領域13及び保守用OS領域12に格納されている古い方の更新ファームウェアを削除していく処理を行っている。

【0091】

次に、図11及び図12の処理フローに従って、管理ハード202の実行する処理について説明する。

【0092】

管理ハード202の主制御機構400は、ACアダプタ203を介して電源が投入されることで起動されると、図11及び図12の処理フローに示すように、先ず最初に、ステップ1で、ファームウェア更新プログラム104や時間監視機構401や本体監視機構402やリモート装置制御ハード204からの通知を待って、通知を受け取ると、ステップ2に進んで、その受け取った通知がファームウェア更新プログラム104の発行する監視時間の通知であるのか否かを判断する。

【0093】

この判断処理により、ファームウェア更新プログラム104の発行する監視時間の通知であること判断するときには、ステップ3に進んで、ファームウェア更新処理中フラグ406をオンすることでファームウェアの適用処理中であることをセットする。

【0094】

続いて、ステップ4で、通知された監視時間を指定して、時間監視機構401に対して時間監視の開始を指示してから、次の通知を待つべくステップ1に戻る。

【0095】

この指示を受け取ると、上述したように、時間監視機構401は、タイマ監視処理に入って、その通知された監視時間の間にファームウェア更新プログラム104から次の監視時間が通知されない場合には、ファームウェア更新プログラム104に異常が発生したことを判断するという処理を行う。

【0096】

一方、ステップ2で、受け取った通知がファームウェア更新プログラム104の発行する監視時間の通知でないことを判断するときには、ステップ5に進んで、その受け取った通知がファームウェア更新プログラム104の発行する監視停止の通知であるのか否かを判断する。

【0097】

この判断処理により、ファームウェア更新プログラム104の発行する監視停止の通知であること判断するときには、ステップ6に進んで、ファームウェア更新処理中フラグ406をオフすることでファームウェアの適用処理中でないことをセットする。

【0098】

続いて、ステップ7で、時間監視機構401に対して時間監視の停止を指示してから、次の通知を待つべくステップ1に戻る。

【0099】

一方、ステップ5で、受け取った通知がファームウェア更新プログラム104の発行する監視停止の通知でないことを判断するときには、ステップ8に進んで、受け取った通知が時間監視機構401の発行するタイムアウトの通知であるのか否かを判断する。

【0100】

この判断処理により、時間監視機構401の検出するタイムアウトの通知であることを判断するときには、ステップ9に進んで、ファームウェア更新処理中フラグ406をオフすることでファームウェアの適用処理中でないことをセットする。

【0101】

続いて、ステップ10で、LAN制御機構404を介して保守管理サーバ2に対して、配信してきた更新ファームウェア103の適用に失敗したことを通知する。なお、このときに適用に失敗した更新ファームウェア103は、システムディスク10の基本OS領域13に保存されており、保守アプリ100の実行する図8の処理フローのステップ5で削除されないことで、次の適用契機に、再び適用対象として設定されることになる。

【0102】

続いて、ステップ11で、基本OS領域13がアクティブになるようにとブート情報を書き換える。すなわち、ファームウェア更新プログラム104がブート情報を書き換えることができないことがある（図9の処理フローのステップ2の前に異常が発生する場合）ことを考慮して、その代わりに、基本OS領域13がアクティブになるようにとブート情報を書き換えるのである。

【0103】

続いて、ステップ12で、ファームウェア更新プログラム104に代わってシステム再立ち上げのリブート処理（リセット処理）を実行してから、次の通知を待つべくステップ1に戻る。

【0104】

一方、ステップ8で、受け取った通知が時間監視機構401の発行するタイムアウトの通知でないことを判断するときには、ステップ13（図12の処理フロー）に進んで、受け取った通知が本体監視機構402の発行する通知（予期せぬ電源切断やリセット指示が発行されたことでファームウェアの適用に失敗したことを知らせる通知）であるのか否かを判断する。

【0105】

この判断処理により、本体監視機構402の発行する通知であることを判断するときには、ステップ14に進んで、ファームウェア更新処理中フラグ406をオフすることでファームウェアの適用処理中でないことをセットする。

【0106】

続いて、ステップ15で、LAN制御機構404を介して保守管理サーバ2に対して、配信してきた更新ファームウェア103の適用に失敗したことを通知し

てから、次の通知を待つべくステップ1に戻る。なお、このときに適用に失敗した更新ファームウェア103は、システムディスク10の基本OS領域13に保存されており、保守アプリ100の実行する図8の処理フローのステップ5で削除されないことで、次の適用契機に、再び適用対象として設定されることになる。

【0107】

一方、ステップ13で、受け取った通知が本体監視機構402の発行する通知でないことを判断するときには、ステップ16に進んで、受け取った通知がファームウェア更新プログラム104の発行する異常検出の通知（図9の処理フローのステップ13で発行される通知）であるのか否かを判断する。

【0108】

この判断処理により、ファームウェア更新プログラム104の発行する異常検出の通知であることを判断するときには、ステップ17に進んで、LAN制御機構404を介して保守管理サーバ2に対して、配信してきた更新ファームウェア103の適用に失敗したことを通知してから、次の通知を待つべくステップ1に戻る。なお、このときに適用に失敗した更新ファームウェア103は、システムディスク10の基本OS領域13に保存されており、保守アプリ100の実行する図8の処理フローのステップ5で削除されないことで、次の適用契機に、再び適用対象として設定されることになる。

【0109】

一方、ステップ16で、受け取った通知がファームウェア更新プログラム104の発行する異常検出の通知でないことを判断するときには、ステップ18に進んで、受け取った通知がリモート装置制御ハード204の発行する装置制御指示の通知（装置制御ハード207に対する電源切断指示やリセット指示の通知）であるのか否かを判断する。

【0110】

この判断処理により、リモート装置制御ハード204の発行する装置制御指示の通知であることを判断するときには、ステップ19に進んで、ファームウェア更新処理中フラグ406がオンしているのか否かを判断して、オフしているとき

には、ステップ 20 に進んで、リモート装置制御ハード 204 の発行する装置制御指示を遮断せずにそのまま装置制御ハード 207 に渡し、オンしているときには、ファームウェア適用処理中に電源切断やリセットがされてしまうとまずいので、その装置制御指示を遮断して装置制御ハード 207 には渡さないようにしてから、次の通知を待つべくステップ 1 に戻る。

【0111】

そして、ステップ 18 で、受け取った通知がリモート装置制御ハード 204 の発行する装置制御指示の通知でないことを判断するときには、ステップ 21 に進んで、通知内容に応じた処理を実行してから、次の通知を待つべくステップ 1 に戻る。

【0112】

このようにして、管理ハード 202 は、ファームウェア更新プログラム 104 の動作を監視して、ファームウェア更新プログラム 104 に異常が発生するときには、保守管理サーバ 2 に対して更新ファームウェア 103 の適用に失敗したことを通知するとともに、ファームウェア更新プログラム 104 の処理を代行して、基本 OS 領域 13 がアクティブになるようにとブート情報を書き換えてから、システム再立ち上げのリブート処理を実行していくように処理するのである。

【0113】

図 13 ないし図 15 に、以上に説明した実施形態例の処理のタイムチャートを図示する。

【0114】

ここで、図 13 は、更新ファームウェア 103 の適用処理が正常に終了したときのタイムチャート、図 14 は、ファームウェア更新プログラム 104 が自分で異常を検出し、更新ファームウェア 103 の適用処理が正常に終了しなかったときのタイムチャート、図 15 は、管理ハード 202 がタイムアウトを検出し、更新ファームウェア 103 の適用処理が正常に終了しなかったときのタイムチャートである。

【0115】

ファームウェア更新プログラム 104 による更新ファームウェア 103 の適用

処理が正常終了する場合には、図13のタイムチャートに示すように、①電源投入で基本OS20が立ち上がり、②保守アプリ100が起動される。

【0116】

このようにして起動されると、保守アプリ100は、(1) ハードウェア構成情報を採取し、(2) その採取したハードウェア構成情報を保守管理サーバ2に送信して、通常の運用処理に入る。

【0117】

そして、(3) 適用契機に到達していないときには何も行わずに通常の適用処理を進め、(4) 保守管理サーバ2から保守資源が配信されてくるときにはそれを受信して、(5) 適用契機に到達すると、(6) 配信されてきた保守資源を保守用OS領域12に格納してから、(7) 保守用OS領域12がアクティブになるようにとブート情報を書き換える。そして、通常の運用処理を続行して、(8) システムを停止させて電源を切断する。

【0118】

その次には、③電源投入で保守用OS30が立ち上がり、④ファームウェア更新プログラム104が起動される。

【0119】

このようにして起動されると、ファームウェア更新プログラム104は、(10) 管理ハード202に対して時間監視を通知してから、(11) 基本OS領域13がアクティブになるようにとブート情報を書き換え、(12) 管理ハード202に対して時間監視を通知してから、(13) 更新ファームウェア103の妥当性をチェックし、(14) 管理ハード202に対して時間監視を通知してから、(15) 更新対象ハードウェアを検索し、(16) 管理ハード202に対して時間監視を通知してから、(17) 更新ファームウェア103と古いファームウェアとを交換し、(18) 管理ハード202に対して監視停止を通知してから、(19) リブート処理を実行して、処理を終了する。

【0120】

そして、その次には、⑤電源投入で基本OS20が立ち上がり、⑥保守アプリ100が起動されることになる。

【0121】

一方、ファームウェア更新プログラム104が自分で異常を検出し、更新ファームウェア103の適用処理が正常に終了しない場合には、図14のタイムチャートに示すように、①電源投入で基本OS20が立ち上がり、②保守アプリ100が起動される。

【0122】

このようにして起動されると、保守アプリ100は、(1)ハードウェア構成情報を採取し、(2)その採取したハードウェア構成情報を保守管理サーバ2に送信して、通常の運用処理に入る。

【0123】

そして、(3)適用契機に到達していないときには何も行わずに通常の適用処理を進め、(4)保守管理サーバ2から保守資源が配信されてくるときにはそれを受信して、(5)適用契機に到達すると、(6)配信されてきた保守資源を保守用OS領域12に格納してから、(7)保守用OS領域12がアクティブになるようにとブート情報を書き換える。そして、通常の運用処理を続行して、(8)システムを停止させて電源を切断する。

【0124】

その次には、③電源投入で保守用OS30が立ち上がり、④ファームウェア更新プログラム104が起動される。

【0125】

このようにして起動されると、ファームウェア更新プログラム104は、(10)管理ハード202に対して時間監視を通知してから、(11)基本OS領域13がアクティブになるようにとブート情報を書き換え、(12)管理ハード202に対して時間監視を通知してから、(13)更新ファームウェア103の妥当性をチェックし、(14)管理ハード202に対して時間監視を通知してから、(15)更新対象ファームウェアを検索し、(16)管理ハード202に対して時間監視を通知してから、(17)更新ファームウェア103を古いファームウェアと交換し、(20)この交換中に異常を検出すると、その旨を管理ハード202に通知する。

【0126】

管理ハード202は、(21)この異常通知を受け取ると、(22)保守管理サーバ2に対して適用失敗を通知する。

【0127】

ファームウェア更新プログラム104は、管理ハード202に対して異常を通知すると、この後、(23)管理ハード202に対して監視停止を通知し、(26)リブート処理を実行して、処理を終了する。

【0128】

そして、その次には、⑤電源投入で基本OS20が立ち上がり、⑥保守アプリ100が起動されることになる。

【0129】

一方、管理ハード202がタイムアウトを検出し、更新ファームウェア103の適用処理が正常に終了しない場合には、図15のタイムチャートに示すように、①電源投入で基本OS20が立ち上がり、②保守アプリ100が起動される。

【0130】

このようにして起動されると、保守アプリ100は、(1)ハードウェア構成情報を採取し、(2)その採取したハードウェア構成情報を保守管理サーバ2に送信して、通常の運用処理に入る。

【0131】

そして、(3)適用契機に到達していないときには何も行わずに通常の適用処理を進め、(4)保守管理サーバ2から保守資源が配信されてくるときにはそれを受信して、(5)適用契機に到達すると、(6)配信されてきた保守資源を保守用OS領域12に格納してから、(7)保守用OS領域12がアクティブになるようにとブート情報を書き換える。そして、通常の運用処理を続行して、(8)システムを停止させて電源を切断する。

【0132】

その次には、③電源投入で保守用OS30が立ち上がり、④ファームウェア更新プログラム104が起動される。

【0133】

このようにして起動されると、ファームウェア更新プログラム104は、(10)

管理ハード 2 0 2 に対して時間監視を通知する。

【 0 1 3 4 】

管理ハード 2 0 2 は、(30)この時間監視の通知を受け取ると、(31)タイマ監視を開始して、(32)タイムアウトを検出すると、(33)保守管理サーバ 2 に対して適用失敗を通知し、(34)基本 OS 領域 1 3 がアクティブになるようにとブート情報を書き換え、(35)リブート処理を実行して、処理を終了する。

【 0 1 3 5 】

そして、その次には、⑤電源投入で基本 OS 2 0 が立ち上がり、⑥保守アプリ 1 0 0 が起動されることになる。

【 0 1 3 6 】

図示実施例に従って本発明を説明したが、本発明はこれに限定されるものではない。例えば、実施例ではファームウェア更新を具体例を本発明を説明したが、本発明はその適用がファームウェアに限られるものではない。

【 0 1 3 7 】

【発明の効果】

以上説明したように、本発明によれば、ネットワークを介して配信されてくる資源を所望の適用契機に自動適用させることが可能になる。

【 0 1 3 8 】

これから、メーカ側は、いちいちサービスマンを派遣する必要がなくなるとともに、資源が更新されたことに気を配らないようなユーザらの苦情を受けずに済むようになる。そして、ユーザは、メーカの提供する更新情報に目を通さなくても、資源を必要なものに更新できるようになる。

【 0 1 3 9 】

更に、この実現にあたって、本発明では、配信されてきた資源の適用処理に失敗しても、通常の運用処理を継続できるようにする構成を採っていることから、通常の運用処理に影響を与えることがない。

【 0 1 4 0 】

更に、この実現にあたって、本発明では、何らかの理由により資源を適用できないことが起こっても、次の適用の機会に再びその資源を適用対象としているの

で、資源を必要なものに確実に更新できるようになる。

【図面の簡単な説明】

【図 1】

本発明の概要構成図である。

【図 2】

本発明の一実施形態例である。

【図 3】

システムディスクのデータ構造の説明図である。

【図 4】

システムディスクのデータ構造の説明図である。

【図 5】

システムディスクのデータ構造の説明図である。

【図 6】

管理ハードとその周辺装置の説明図である。

【図 7】

管理ハードの持つハードウェア機構の一実施形態例である。

【図 8】

保守アプリの実行する処理フローの一実施形態例である。

【図 9】

ファームウェア更新プログラムの実行する処理フローの一実施形態例である。

【図 1 0】

ファームウェア更新プログラムの実行する処理フローの一実施形態例である。

【図 1 1】

管理ハードの実行する処理フローの一実施形態例である。

【図 1 2】

管理ハードの実行する処理フローの一実施形態例である。

【図 1 3】

実施形態例のタイムチャートである。

【図 1 4】

実施形態例のタイムチャートである。

【図 15】

実施形態例のタイムチャートである。

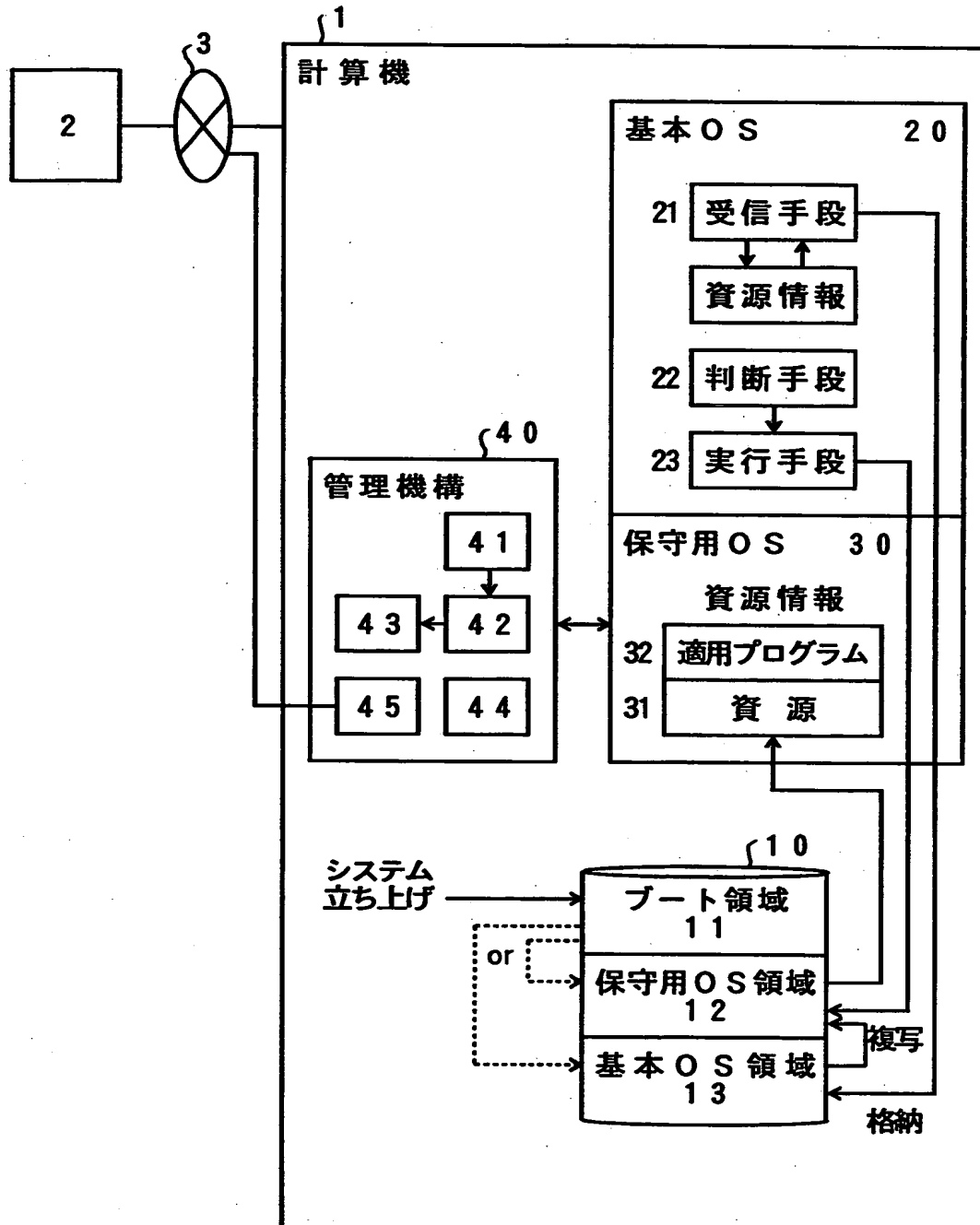
【符号の説明】

- 1 計算機
- 2 保守管理サーバ
- 3 ネットワーク
- 10 システムディスク
- 11 ブート領域
- 12 保守用OS領域
- 13 基本OS領域
- 20 基本OS
- 21 受信手段
- 22 判断手段
- 23 実行手段
- 30 保守用OS
- 31 資源
- 32 適用プログラム
- 40 管理機構
- 41 監視手段
- 42 書換手段
- 43 再立ち上げ手段
- 44 無効化手段
- 45 通知手段

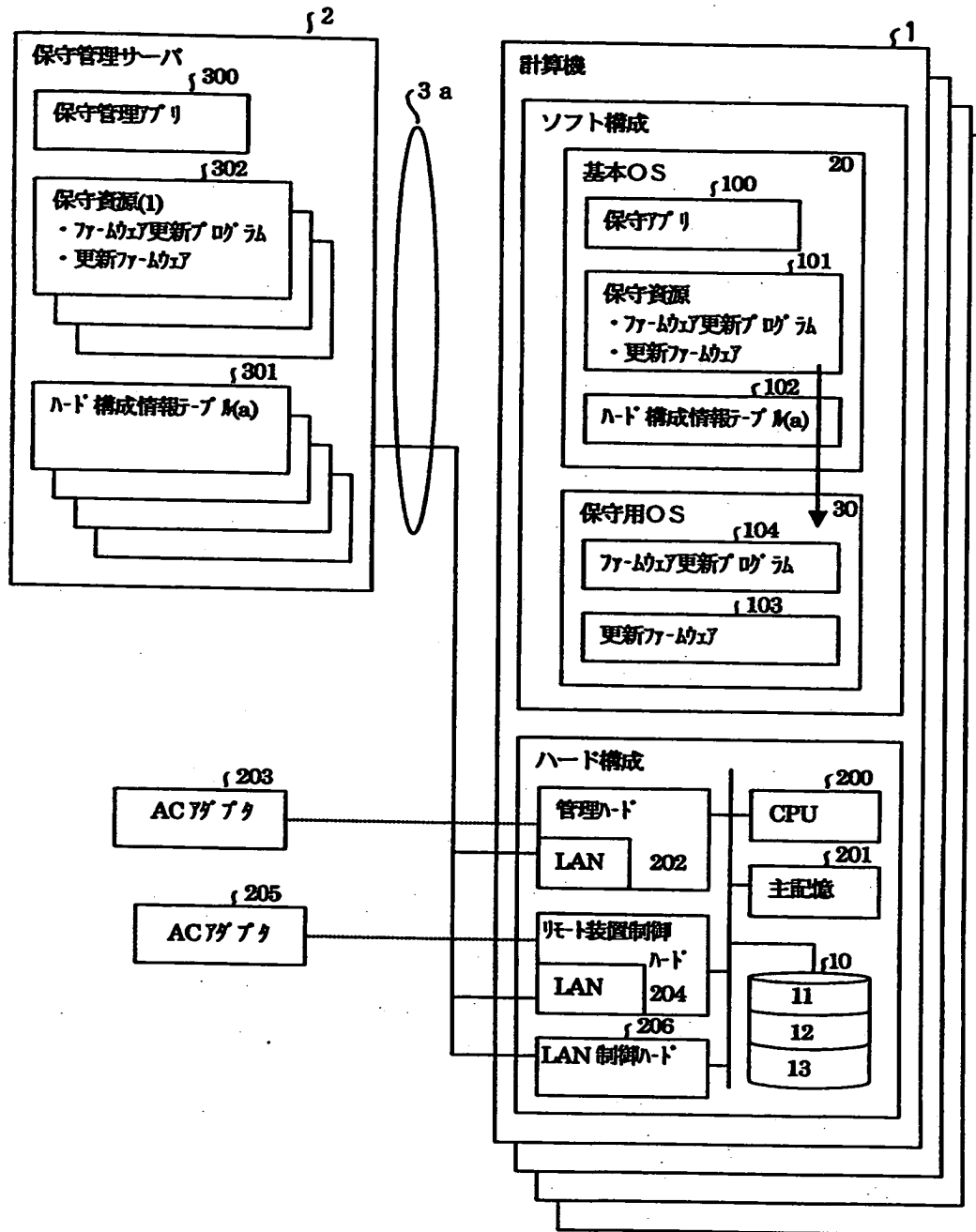
【書類名】

図面

【図 1】



【図 2】



【図3】

ブートセクタ (512バイト)
ファイルアロケーションテーブル1
ファイルアロケーションテーブル2
ルートディレクトリ
保守用OS領域
基本OS領域

(a)

0x000	JMP命令
0x003	OEM識別フィールド
0x00B	BIOSパラメータブロック
0x03C	ブートストラップローダ
0x1BE	パーティションテーブル
0x1FE	ブート認証ワード (0xAA55)

(b)

	+0	+1	+2	+3	+4	+5	+6	+7	+8~+11	+12~+15
0x1BE	BI	H	S	C	SI	H	S	C	SP	N
0x1CE	BI	H	S	C	SI	H	S	C	SP	N
0x1DE	BI	H	S	C	SI	H	S	C	SP	N
0x1EE	BI	H	S	C	SI	H	S	C	SP	N

(c)

【図 4】

オフセット	サイズ	記号	内容
+0	1 バイト	BI	ブートインディケータ 0x80: アクティープパーティション
+1~+4	3 バイト	H/S/C	始点のヘッド番号/セクタ番号/シリンダ番号
+4	1 バイト	SI	システムインディケータ
+5~+7	3 バイト	H/S/C	終点のヘッド番号/セクタ番号/シリンダ番号
+8~+11	4 バイト	SP	前パーティションセクタ数
+12~+15	4 バイト	N	自パーティションセクタ数

【図 5】

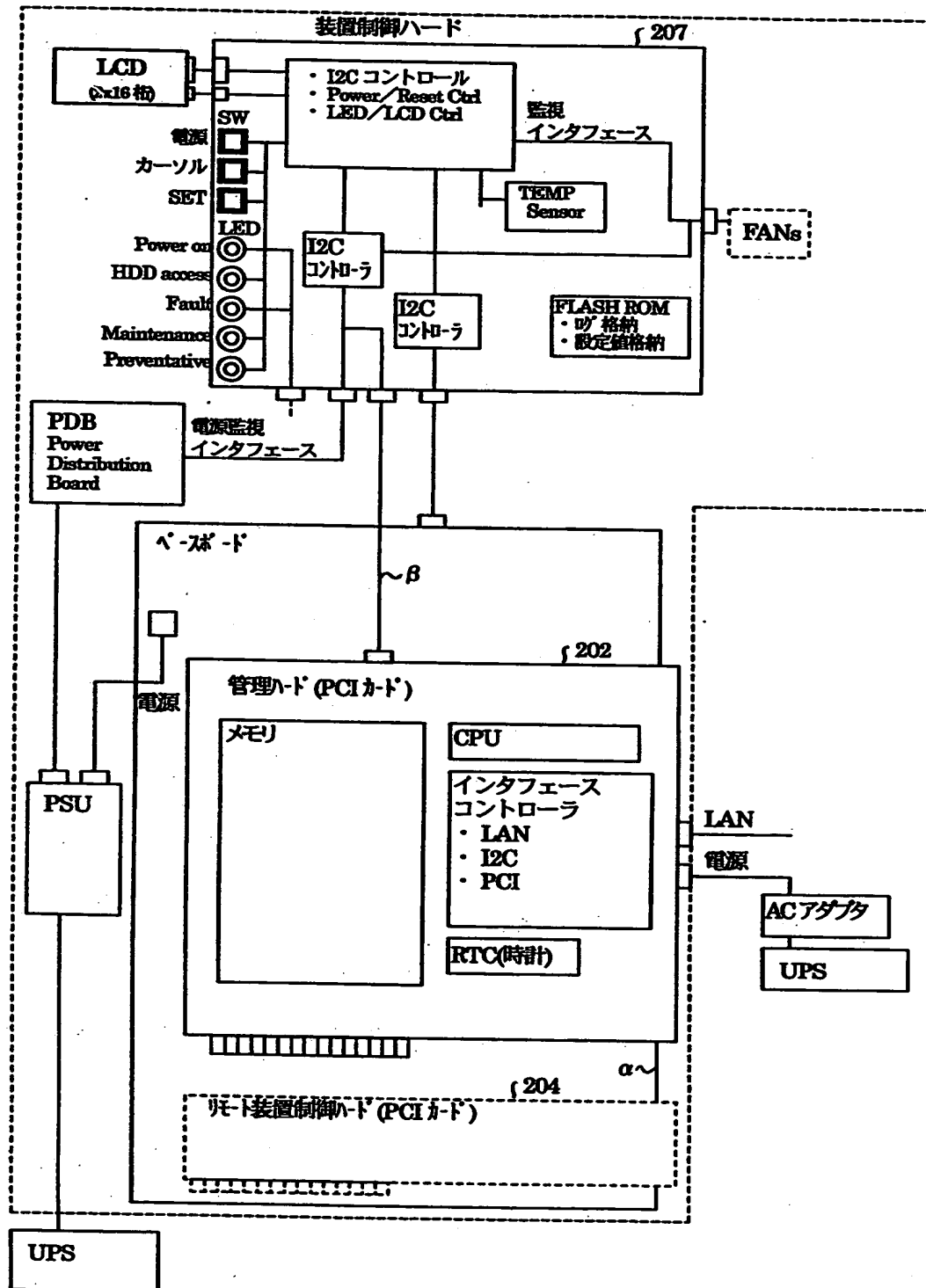
	+0 BI	+1~+3 H/S/C	+4 SI	+5~+7 H/S/C	+8~+11 SP	+12~+15 N
0x1BE	0x00	0xXXXXXXXX	0xXX	0xXXXXXXXX	0xXXXXXXXXXX	0xXXXXXXXXXX
0x1CE	0x80	0xXXXXXXXX	0xXX	0xXXXXXXXX	0xXXXXXXXXXX	0xXXXXXXXXXX

(a)

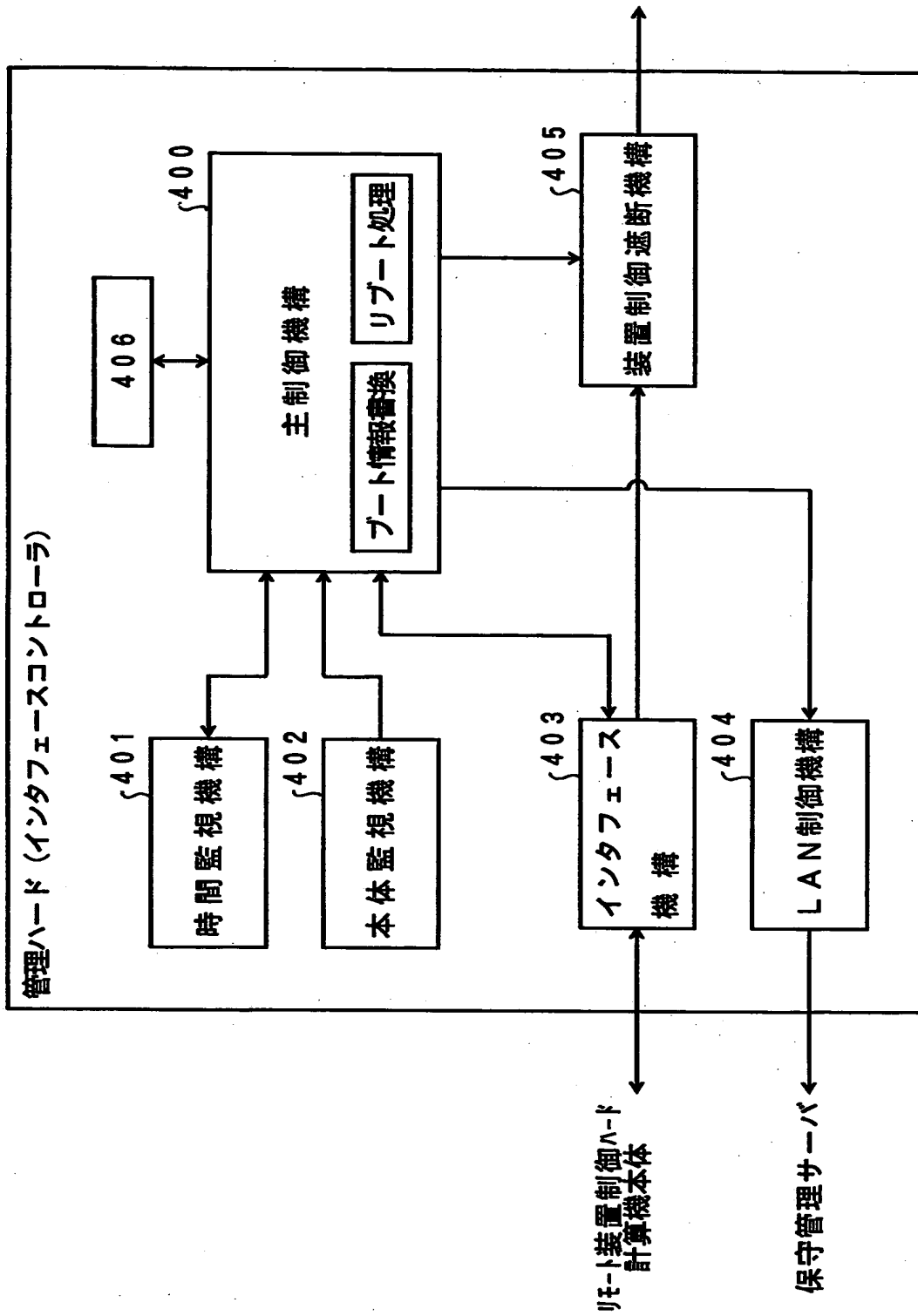
	+0 BI	+1~+3 H/S/C	+4 SI	+5~+7 H/S/C	+8~+11 SP	+12~+15 N
0x1BE	0x80	0xXXXXXXXX	0xXX	0xXXXXXXXX	0xXXXXXXXXXX	0xXXXXXXXXXX
0x1CE	0x00	0xXXXXXXXX	0xXX	0xXXXXXXXX	0xXXXXXXXXXX	0xXXXXXXXXXX

(b)

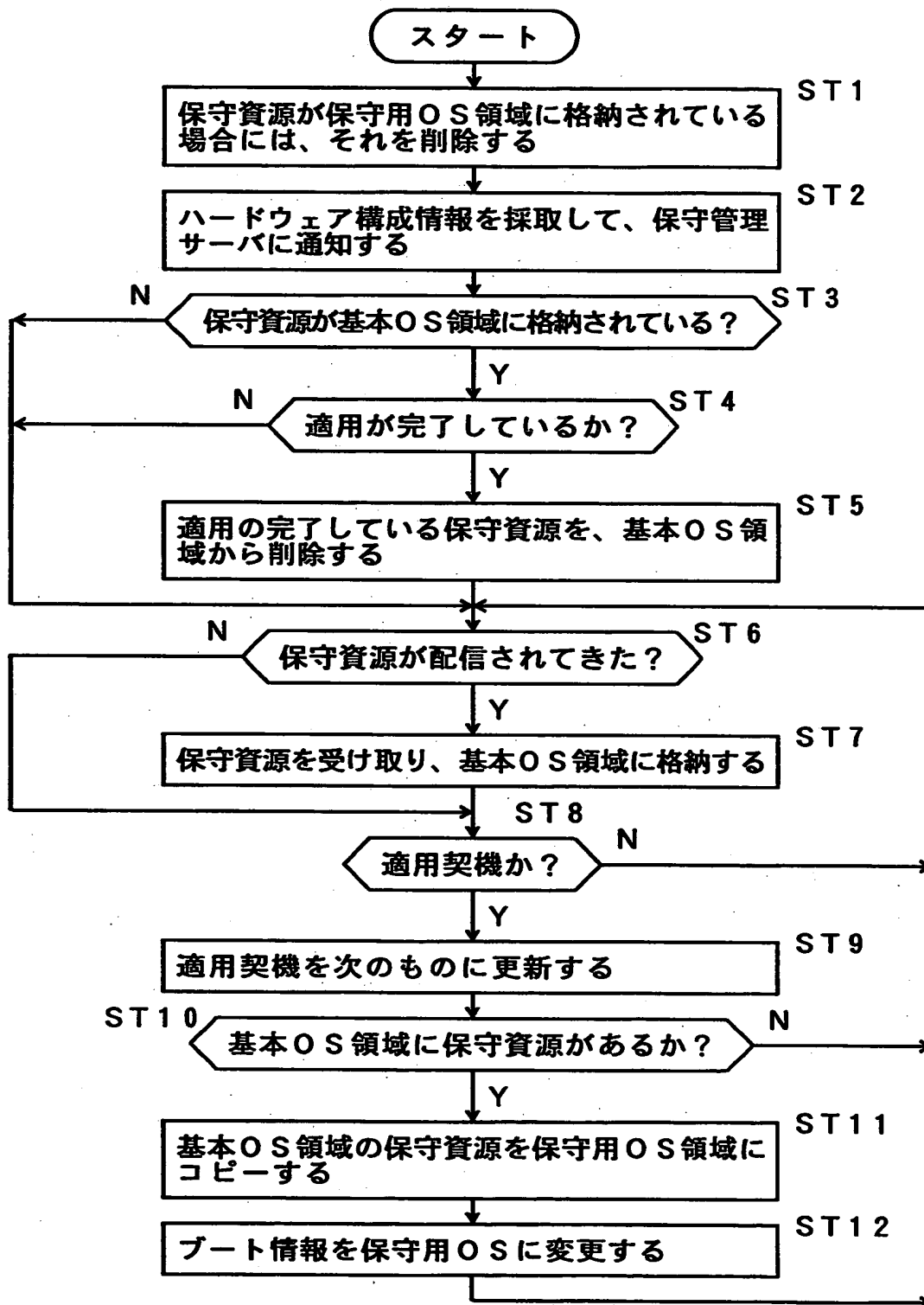
【図 6】



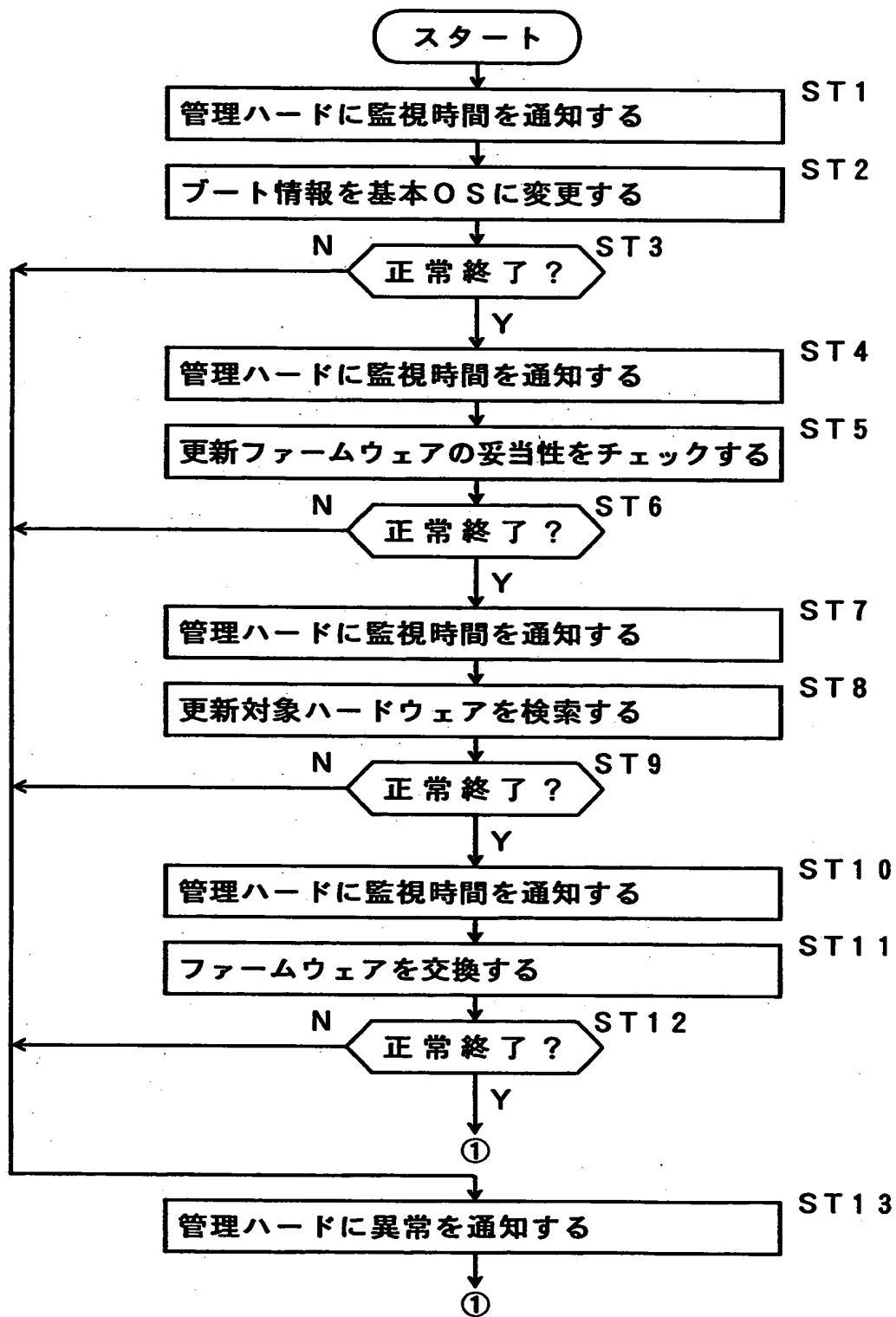
【図 7】



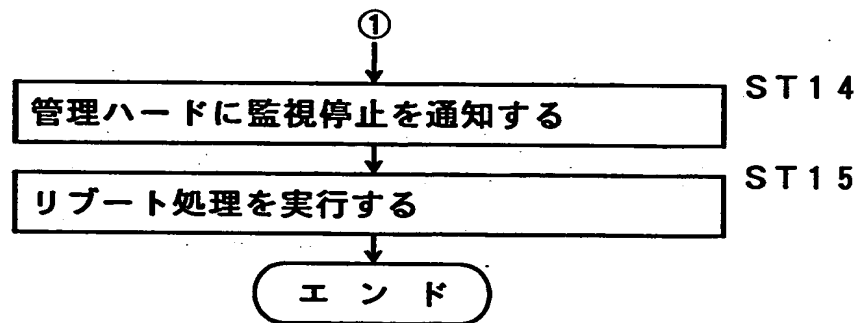
【図 8】



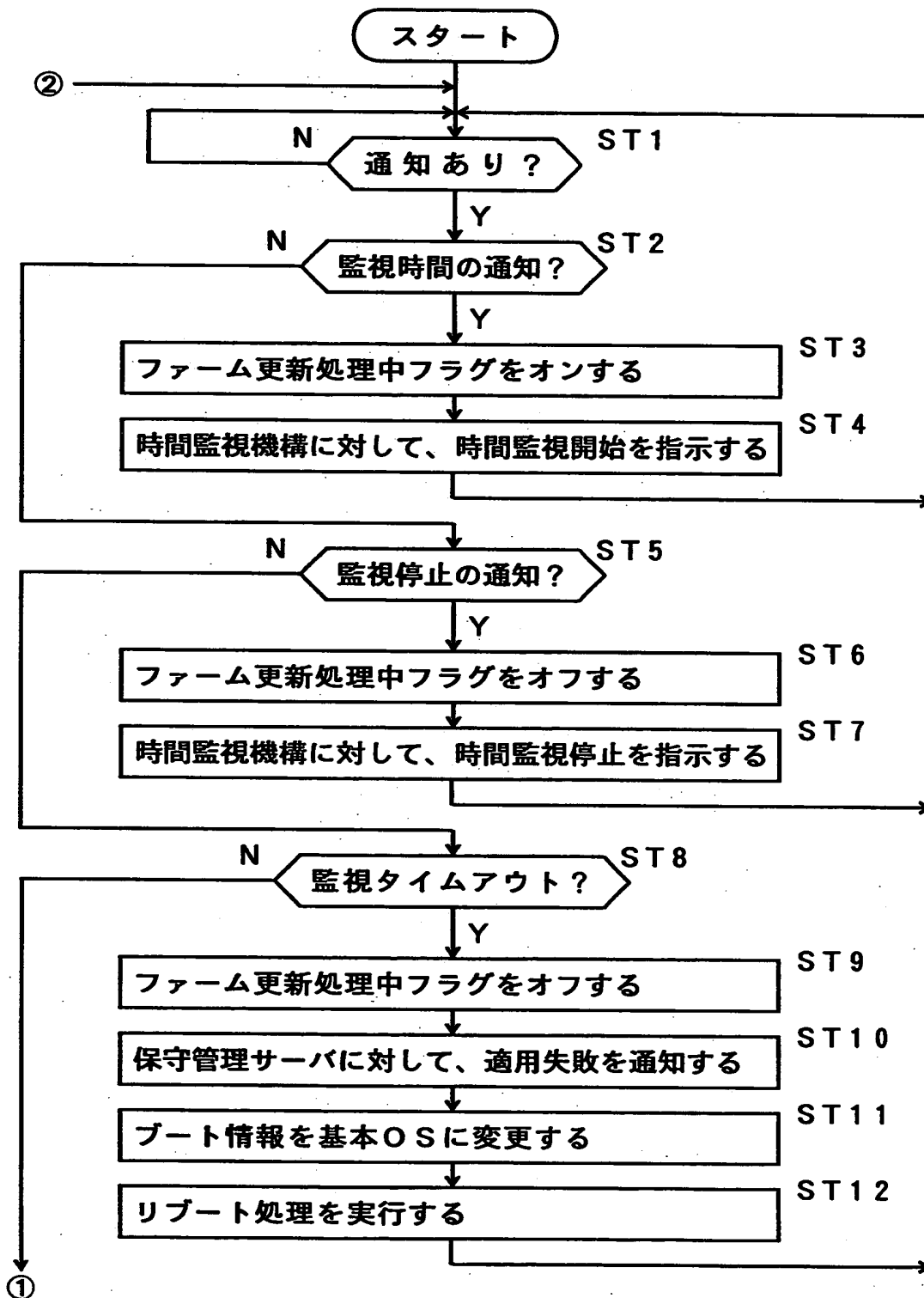
【図9】



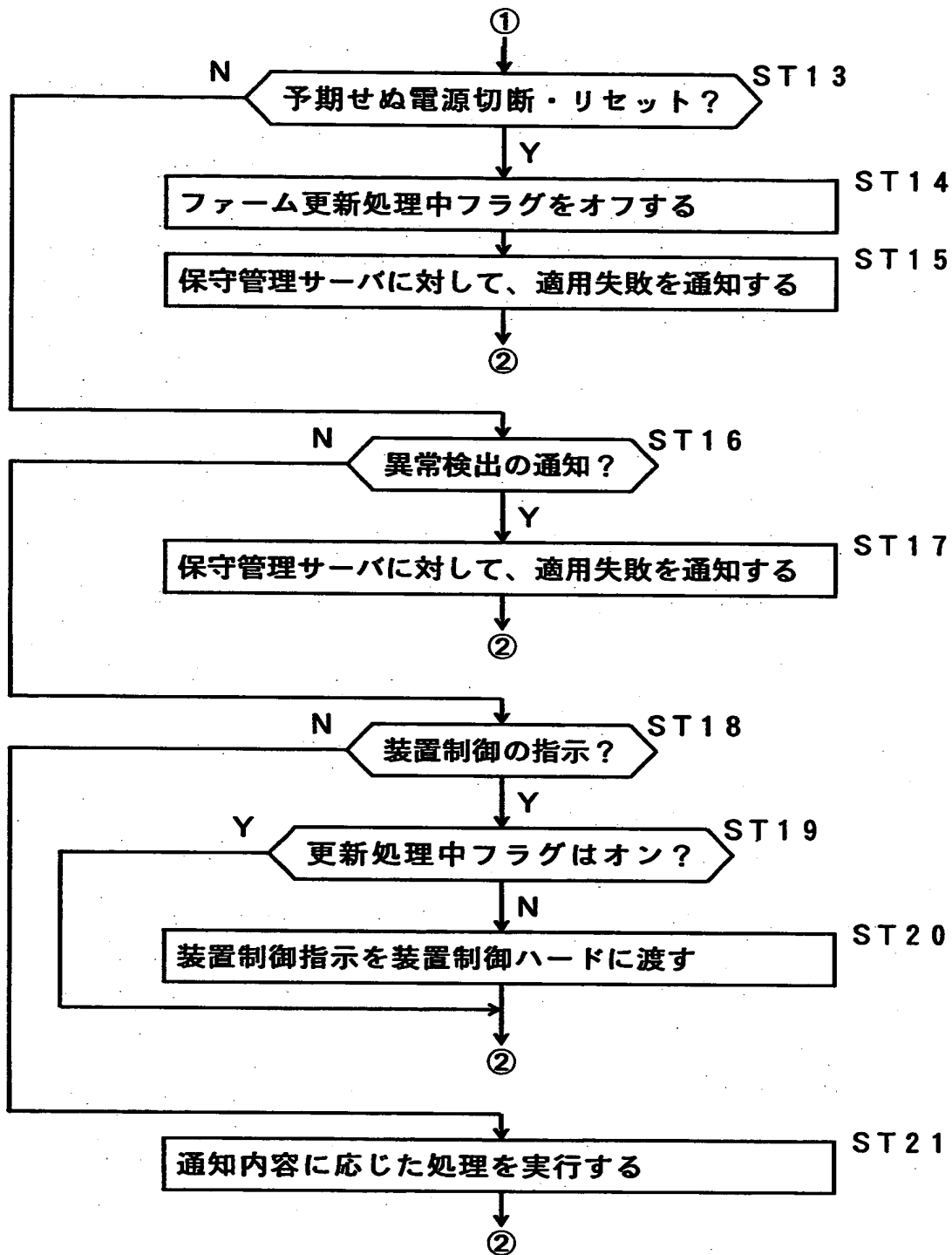
【図10】



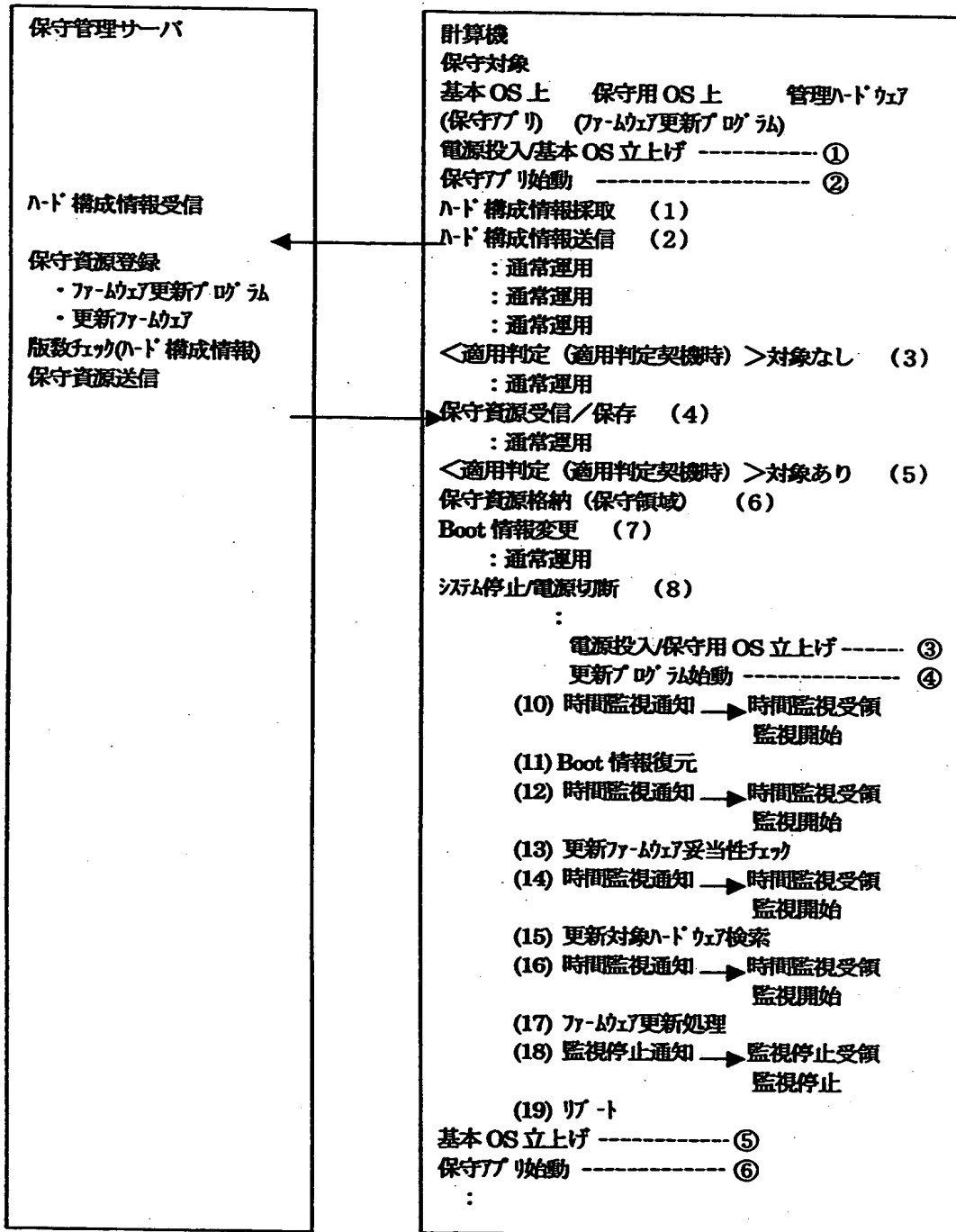
【図11】



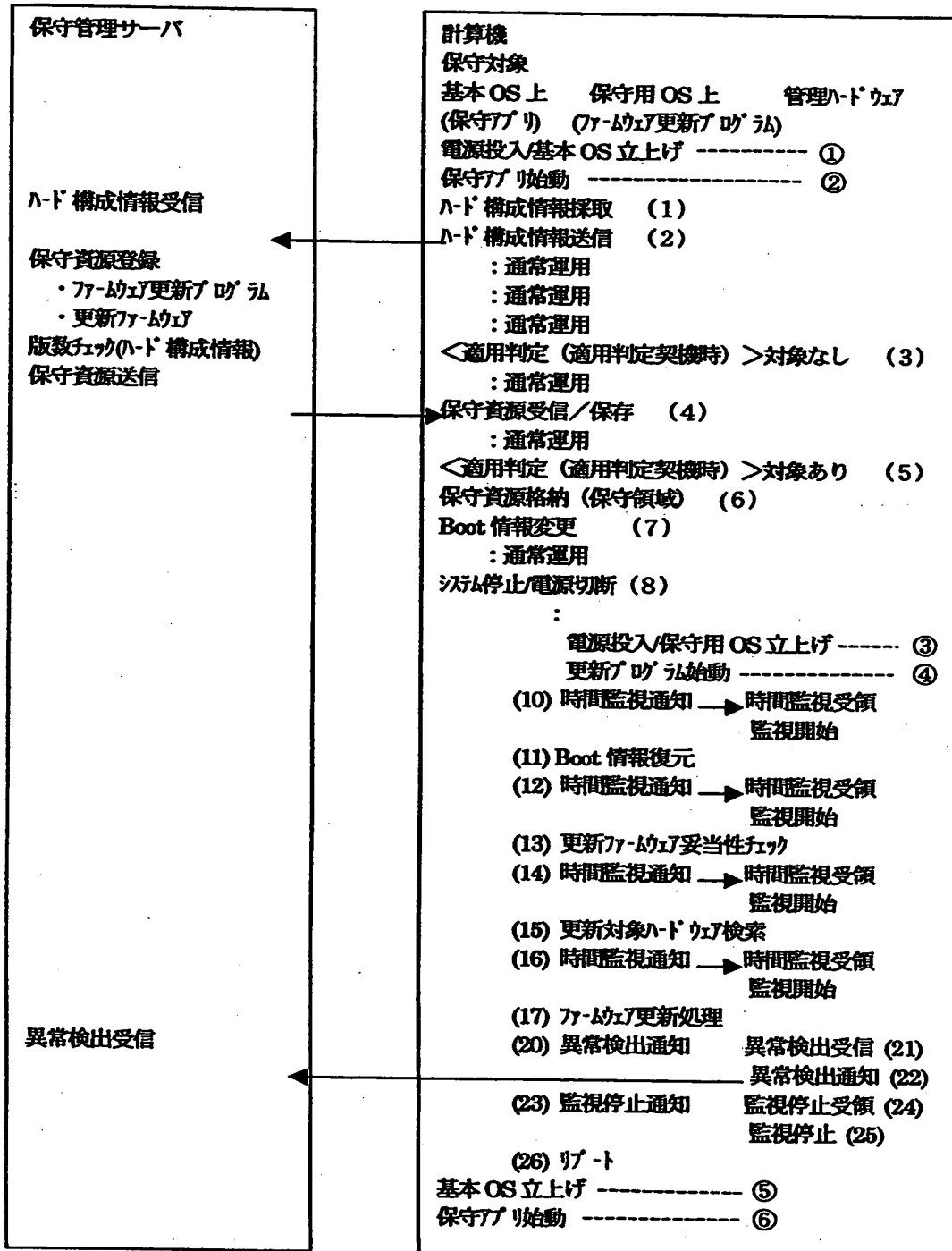
【図12】



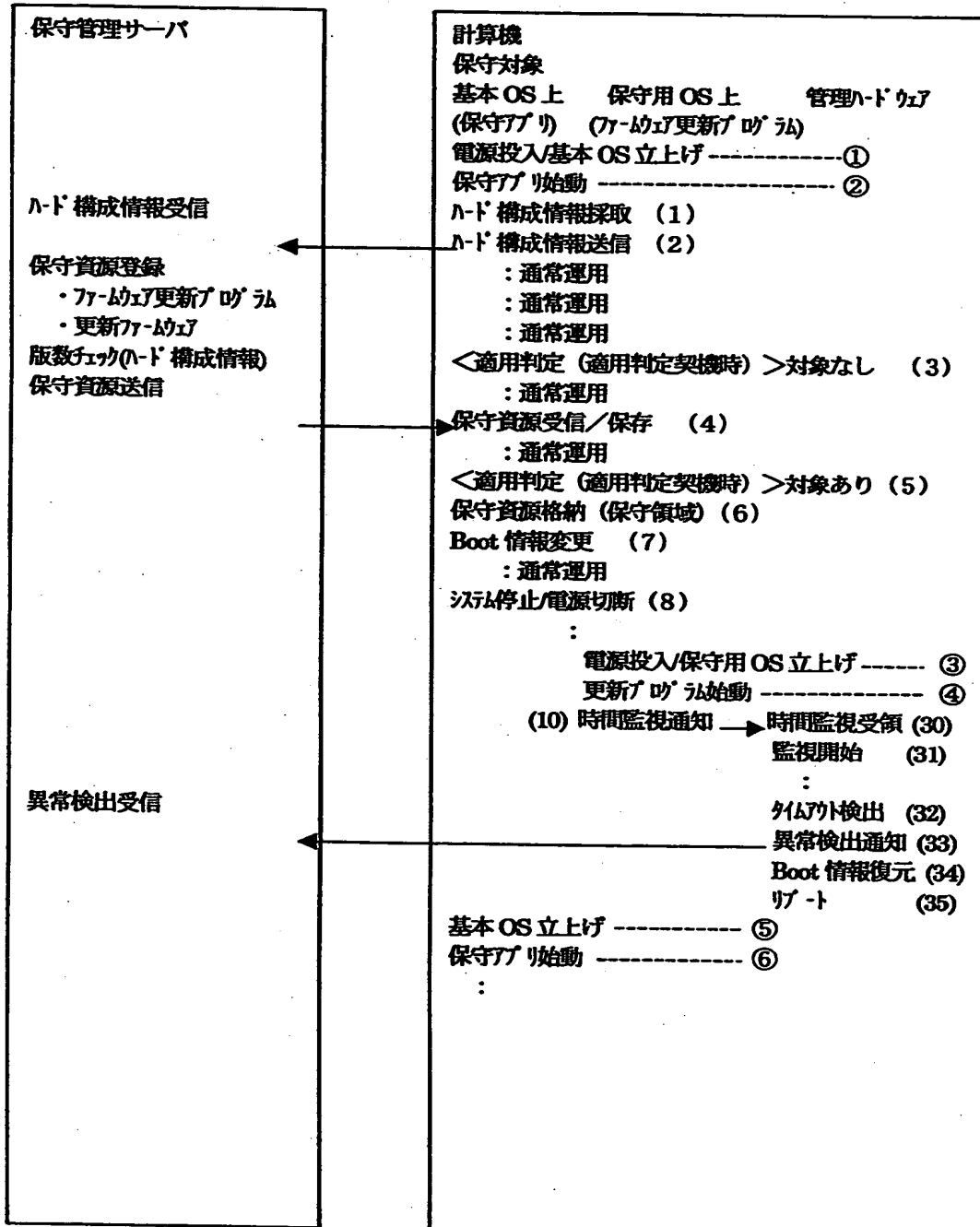
【図 13】



【図 14】



【図15】



【書類名】 要約書

【要約】

【課題】 本発明は、ネットワークを介して配信されてくる資源を所望の適用契機に自動適用させることを可能にする計算機の提供を目的とする。

【解決手段】 ネットワークを介して送られてくる、資源とそれを適用させるための適用プログラムとで構成される資源情報を受信し、記憶装置の運用領域に格納する手段と、その資源の適用契機に到達したのか否かを判断する手段と、適用契機に到達したことを判断する場合に、その資源情報を記憶装置の保守領域に複写するとともに、次回のシステム立ち上げ時に保守領域が有効化されることになるための処理を行う手段とを備えるように構成する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社